Procedure: No. 2205.03: Computer Virus Protection
Reference: Policy 2205
Effective: 01/01/05
Prior Issue: N/A

Purpose:

In an effort to safeguard networks and critically sensitive information from software contaminants, Arizona Department of Juvenile Corrections (ADJC) Management Information Systems (MIS) shall implement an architecture that protects against the following but is not limited to:

- Boot sector Viruses;
- File Infectors;
- Macro Viruses;
- Stealth Viruses;
- Polymorphic Viruses;
- Multipartite Viruses;
- Worms;
- Trojan Horses;
- Spy Ware;
- Adware;
- Key loggers;
- Other types of malicious code.

MIS shall also implement a protection architecture that guards against intrusion via the use of Instant Messaging provided by services. The Instant Messenger attachments typically bypass firewalls or gateways that scan for malicious content; if the content is encrypted either through the use of secure socket layer (SSL) or Virtual Private Network services, detection is more difficult.

Rules:

1. **MANAGEMENT INFORMATION SYSTEMS (MIS) EMPLOYEES** shall develop in accordance to GITA Policy P800-S860 an anti-virus system to protect all systems connected to the ADJC network.
   a. Anti-virus system shall be an automated process:
      i. Anti-virus updates are to be checked nightly and replicated out to all networked devices:
      ii. Anti-Virus software shall not be enabled for the user to circumvent;
      iii. Anti-Virus software shall be able to "clean and notify" when a virus or malicious code is detected on a network system;
      iv. MIS shall notify SIPC (State Information Protection Center) within one hour of being notified that a virus has been detected on the ADJC network;
         (1) SIPC Form (F2205.03A) shall be used for notification;
      v. Anti-Virus software shall be placed into a real time scanning mode to scan all information accessed on network devices;
      vi. All incoming email shall be scanned for open relay servers, viruses, malicious code, and content scanned for keywords and offensive language;
      vii. Computer updates shall be applied quarterly to network systems to prevent security holes that virus's and malicious code exploit;
      viii. All patches/hot-fixes recommended by the equipment vendor and MIS shall be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. MIS shall continue to develop processes to put in place to stay current on appropriate patches/hot fixes.

2. **MANAGEMENT INFORMATION SYSTEMS (MIS) SECTION** shall provide instruction to agency employees concerning protecting their computer against a computer virus.

3. To prevent viruses from infecting the Department's local and wide area network system, the **AGENCY EMPLOYEE** shall take the following precautionary steps:
   a. Allow the virus protection/detection software to scan on a regular basis. The anti-virus system shall scan weekly automatically. Do not cancel the scan of the system;
   b. Contact MIS for assistance:
      i. If the anti-virus program finds a virus and did not clean the virus from your computer or
      ii. If the same virus occurs repeatedly,;
   c. Do not disable settings such as Real time Protection and weekly scan on the Anti-virus software;
   d. Do not install software without prior approval from MIS;
   e. Do not use or permit installation of pirated/illegal copies of software. Only licensed or agency sanctioned software should be installed on Department computers;
   f. Use caution when obtaining files from the Internet or from email when the source or sender cannot be verified.

4. The **AGENCY EMPLOYEES** shall stop any computer work and notify MIS immediately when their computer notifies them that it has a virus.

5. **MIS** shall repair immediately virus or malicious code infections by applying patches directly on the infected machine upon notification.
   a. **MIS** shall use automated systems for patch management when deemed appropriate. This automated system can be used for deploying software, as well as updates to the computers operating system, and/or applications on the computer system.

Effective Date:	Approved by Process Owner:	Review Date:	Reviewed By: